

- EPODOC / EPO

PN - JP2000004226 A 20000107
PD - 2000-01-07
PR - JP19980167300 19980615
OPD - 1998-06-15
TI - COMMUNICATION DATA CONCEALING SYSTEM
IN - HIRAYAMA HIROYUKI; KANEKO KIYOSHI
PA - FUJITSU LTD
IC - H04L9/36 ; H04L12/40 ; H04L12/56
- WPI / DERWENT

TI - Secret data communication system for use in internet, uses predetermined key and numerical value to encrypt data to be transmitted

PR - JP19980167300 19980615
PN - JP2000004226 A 20000107 DW200046 H04L9/36 021pp
PA - (FUIT) FUJITSU LTD
IC - H04L9/36 ;H04L12/40 ;H04L12/56
AB - JP2000004226 NOVELTY - At the transmission side, an

encryption unit divides the communication data to predetermined length and encrypts and adds a numerical value to each divided data according to a predetermined key. The numerical value shows division technique or division offset of each data. The data is then transmitted to a receiving terminal where the data is decoded using the predetermined key and numerical value.

- USE - For secret data communication in internet.

- ADVANTAGE - Secrecy of data can be maintained effectively due to the addition of numerical value.

- (Dwg.1/19)

OPD - 1998-06-15
AN - 2000-507738 [46]
- PAJ / JPO

PN - JP2000004226 A 20000107
PD - 2000-01-07
AP - JP19980167300 19980615
IN - KANEKO KIYOSHI;HIRAYAMA HIROYUKI
PA - FUJITSU LTD
TI - COMMUNICATION DATA CONCEALING SYSTEM
AB - PROBLEM TO BE SOLVED: To provide a communication data concealing system capable of concealing the contents of communication data by scrambling these communication data so as not to know the contents of entire communication data even when the communication data are monitored on a network.

- SOLUTION: In this communication data concealing system, communication data are divided into prescribed data length, a numerical value showing the order or offset of respective divided data is enciphered while using a prescribed key, the divided data are sent to the network while adding this value, the enciphered numerical value added to the respective divided data received from the network is deciphered while using a prescribed key and according to the order or offset shown by the deciphered numerical value, the source communication data are restored from the received divided data. Thus, even when the communication data are monitored on the network, these communication data are scrambled for the prescribed data length, the contents of entire communication data can not be known and the contents of communication data can be concealed.

I - H04L9/36 ;H04L12/40 ;H04L12/56

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-4226

(P2000-4226A)

(43) 公開日 平成12年1月7日 (2000.1.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L	9/36	H 0 4 L 9/00	6 8 5 5 K 0 1 3
	12/40	11/00	3 2 0 5 K 0 3 0
	12/56	11/20	1 0 2 Z 5 K 0 3 2

審査請求 未請求 請求項の数 5 O L (全 21 頁)

(21) 出願番号 特願平10-167300

(22) 出願日 平成10年6月15日 (1998.6.15)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(72) 発明者 金子 清

神奈川県川崎市高津区坂戸3丁目2番1号
富士通ネットワークエンジニアリング株式会社内

(74) 代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

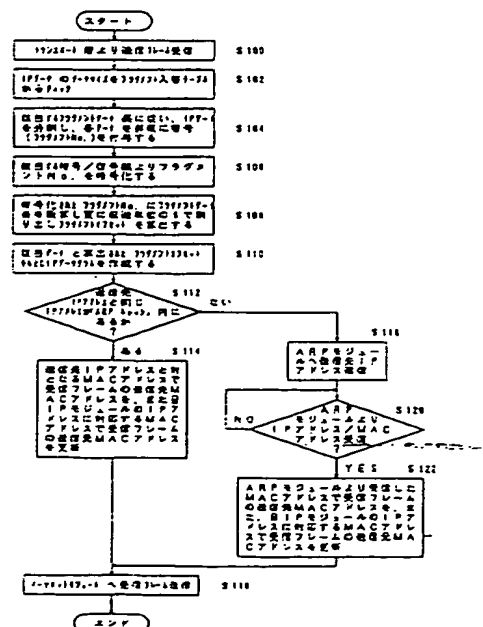
(54) 【発明の名称】 通信データ秘匿方式

(57) 【要約】

【課題】 ネットワーク上で通信データをモニタしたとしても、この通信データがスクランブルされて通信データ全体の内容を知ることができず、通信データの内容を秘匿できる通信データ秘匿方式を提供することを目的とする。

【解決手段】 通信データを所定データ長に分割し、分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して分割データそれぞれに付加しネットワークに送出し、ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って受信した分割データから元の通信データを復元するため、ネットワーク上で通信データをモニタしたとしても、この通信データが所定データ長でスクランブルされており、通信データ全体の内容を知ることができず、通信データの内容を秘匿できる。

データ送信元のIPモジュール24が行う送信動作のフローチャート



【特許請求の範囲】

【請求項1】 送信側の端末に、通信データを所定データ長に分割し、前記分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して前記分割データそれぞれに付加しネットワークに送出する暗号化手段を設け、

受信側の端末に、前記ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を前記所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って前記受信した分割データから元の通信データを復元する復号化手段を設け、

前記ネットワーク上で通信データの内容を秘匿することを特徴とする通信データ秘匿方式。

【請求項2】 請求項1記載の通信データ秘匿方式において、

前記暗号化手段及び復号化手段で用いる所定の鍵は、前記通信データのデータ長に対応して決定することを特徴とする通信データ秘匿方式。

【請求項3】 請求項2記載の通信データ秘匿方式において、

前記通信データを分割する所定データ長は、前記通信データのデータ長に対応して決定することを特徴とする通信データ秘匿方式。

【請求項4】 請求項1乃至3のいずれか記載の通信データ秘匿方式において、

前記送信側及び受信側の端末は、TCP/IPプロトコルに基づいてネットワークと通信を行うことを特徴とする通信データ秘匿方式。

【請求項5】 請求項1乃至3のいずれか記載の通信データ秘匿方式において、

前記送信側及び受信側の端末は、X.25プロトコルに基づいてネットワークと通信を行うことを特徴とする通信データ秘匿方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は通信データ秘匿方式に関し、インターネットで伝送される通信データの内容が第三者に知られないようにする通信データ秘匿方式に関する。

【0002】

【従来の技術】インターネット上を流れる通信データは通常一つのデータグラムか複数のデータグラムに分割されて伝送される。図1はTCP/IPをサポートした端末の機能ブロック図を示す。同図中、イーサネットモジュール10はCSMA/CD(搬送波感知多重アクセス/衝突検出)方式によりネットワーク12とイーサネットフレームの送信/受信を行い、ネットワークより受信したイーサネットフレームをIP層のIPモジュール14、ARPモジュール16に送信し、IP層から受信したイーサネットフレームをネットワーク12に送信す

る。その動作フローチャートを図2に示す。

【0003】ARPキャッシュ18は接続されている各ネットワーク内の各ノードのIPアドレスとMAC(媒体アクセス制御)アドレスを図3に示すように各ノード毎に對て保持している。ARPモジュール16はIPモジュール14からIPアドレスを受信すると、当該IPアドレスを送信先IPアドレスとしてARPデータグラム(ARP要求)を作成しイーサネットモジュール10に送信する。また、イーサネットモジュール10よりARPデータグラム(ARP応答)を受信すると、ARPデータグラム(ARP応答)内の送信元IPアドレスとMACアドレスをIPモジュール14に送信すると共にARPキャッシュ18に登録する。その動作フローチャートを図4に示す。

【0004】IPモジュール14はIPデータグラムを送信する場合、トランスポート層20から受信したIPデータグラムのサイズがネットワークのITU(最大転送単位)を超える場合IP層によるデータグラムの分割であるフラグメンテーションを行う。そして、送信先IPアドレスに含まれるネットワークアドレスと、自IPモジュールの保持しているIPアドレスに含まれるネットワークアドレスとを比較チェックする。一致すれば送信先IPアドレスと同一IPアドレスを持つデータエントリをARPキャッシュ18より検索し、当該データのMACアドレスでイーサネットフレーム内の送信先MACアドレスを更新しイーサネットモジュール10に送信する。

【0005】同一IPアドレスを持つデータエントリがない場合はARPモジュール16に送信先IPアドレスを送信し、ARPモジュール16より対応する送信先IPアドレスとMACアドレスを受信した後、イーサネットフレーム内の送信先MACアドレスを更新しイーサネットモジュール10に送信する。その送信の動作フローチャートを図5に示す。

【0006】イーサネットモジュール10よりIPデータグラムを受信した場合、受信したIPアドレスと自IPアドレスを比較し、一致していればIPデータグラム内のモアビットを参照し、フレーム分割されているならば全フレームを受信しフラグメンテーションにより元のデータグラムの再構築を行い、トランスポート層20にIPデータグラムを送信する。IPアドレスが不一致の場合は、イーサネットフレームを破棄する。その受信の動作フローチャートを図6に示す。

【0007】図7にイーサネットフレームのIPデータグラムのフレームフォーマットを示す。同図中、FLAG(3ビット)はフラグメンテーションの制御に使用され、FLAGのLSBはモアフラグと呼ばれ、0であればデータグラムの最後を示す。第2ビットはフラグメント禁止ビットである。フラグメントオフセット(13ビット)はフラグメントされたデータが分割前のメッセージ

のどの位置を占めるのかを示す、なお、フラグメントは8オクテット単位で行われる。

【0008】ここで、図8に示すネットワーク1のMTU(単位はオクテット)は1200、ネットワーク2のMTUは532、ネットワーク3のMTUは276であるとする。ノード発信元でオリジナルのデータグラムが1024オクテットのデータを持つ場合、ノード発信元ではフラグメント無しでデータグラムを送信する。ルータAではネットワーク2のMTUが532であるため、上記データグラムを512オクテットのデータを持つ2つのデータグラムに分離して送信する。また、ルータBではネットワーク3のMTUが276であるため、上記2つのデータグラムを256オクテットのデータを持つ4つのデータグラムに分離して送信する。エンドノードではフラグメントされた全てのデータグラムを受信して元のデータグラムを再構築する。

【0009】

【発明が解決しようとする課題】インターネット上を流れる通信データは前述のように、一つのデータグラムが複数のデータグラムに分割されて伝送されるが、TCP/IP(トランスミッション コントロール プロトコル/インターネット プロトコル)ではデータ秘匿に関するプロトコル上のサポートが無く平文のままデータが伝送されている。

【0010】このため、通信データの秘匿性を考慮すると、通信データの内容を知りうる権限のない第三者でも、通信ルート上のルータ等によりIPデータのモニタが可能であれば、任意のIPデータグラムを収集可能である。この場合、秘匿性を要する情報がフラグメンテーションで複数のIPデータグラムに分割されて通信されていたとしても、平文のデータが通信されているために分割された複数のIPデータグラムを取り込み再構築することにより、通信データ全体の内容を知り得てしまうという問題があった。

【0011】本発明は上記の点に鑑みなされたもので、ネットワーク上で通信データをモニタしたとしても、この通信データがスクランブルされて通信データ全体の内容を知ることができず、通信データの内容を秘匿できる通信データ秘匿方式を提供することを目的とする。

【0012】

【課題を解決するための手段】請求項1に記載の発明は、送信側の端末に、通信データを所定データ長に分割し、前記分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して前記分割データそれぞれに付加しネットワークに送出する暗号化手段を設け、受信側の端末に、前記ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を前記所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って前記受信した分割データから元の通信データを復元する復号化手段を設け、前

記ネットワーク上で通信データの内容を秘匿する。

【0013】このように、通信データを所定データ長に分割し、分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して分割データそれぞれに付加しネットワークに送出し、ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って受信した分割データから元の通信データを復元するため、ネットワーク上で通信データをモニタしたとしても、この通信データが所定データ長でスクランブルされており、通信データ全体の内容を知ることができず、通信データの内容を秘匿できる。

【0014】請求項2に記載の発明は、請求項1記載の通信データ秘匿方式において、前記暗号化手段及び復号化手段で用いる所定の鍵は、前記通信データのデータ長に対応して決定する。このように、所定の鍵を通信データのデータ長に対応して決定するため、送信側、受信側それぞれで同一の鍵を用いて暗号化、復号化を行うことができ、かつ、鍵を送信しないためにデータ秘匿性が向上する。

【0015】請求項3に記載の発明は、請求項2記載の通信データ秘匿方式において、前記通信データを分割する所定データ長は、前記通信データのデータ長に対応して決定する。このように、所定データ長を通信データのデータ長に対応して決定するため、受信側では受信した分割データのデータ長から一意に復号化の鍵を知ることができる。

【0016】請求項4に記載の発明は、請求項1乃至3のいずれか記載の通信データ秘匿方式において、前記送信側及び受信側の端末は、TCP/IPプロトコルに基づいてネットワークと通信を行う。これによって、TCP/IPプロトコルの通信において通信データの秘匿性を得ることができる。

【0017】請求項5に記載の発明は、請求項1乃至3のいずれか記載の通信データ秘匿方式において、前記送信側及び受信側の端末は、X.25プロトコルに基づいてネットワークと通信を行う。これによって、X.25プロトコルの通信において通信データの秘匿性を得ることができる。

【0018】

【発明の実施の形態】図9は本発明の通信データ秘匿方式を適用したTCP/IPをサポートした端末の機能ブロック図を示す。同図中、図1と同一部分には同一符号を付す。図9において、イーサネットモジュール10はCSMA/CD(搬送波感知多重アクセス/衝突検出)方式によりネットワーク12とイーサネットフレームの送信/受信を行い、ネットワークより受信したイーサネットフレームをIP層のIPモジュール24、ARPモジュール16に送信し、IP層から受信したイーサネッ

トフレームをネットワーク12に送信する。その動作フローチャートを図2に示す。

【0019】ARPキャッシュ18は接続されている各ネットワーク内の各ノードのIPアドレスとMAC（媒体アクセス制御）アドレスを図3に示すように各ノード毎に保持している。ARPモジュール16はIPモジュール24からIPアドレスを受信すると、当該IPアドレスを送信先IPアドレスとしてARPデータグラム（ARP要求）を作成しイーサネットモジュール10に送信する。また、イーサネットモジュール10よりARPデータグラム（ARP応答）を受信すると、ARPデータグラム（ARP応答）内の送信元IPアドレスとMACアドレスをIPモジュール24に送信すると共にARPキャッシュ18に登録する。その動作フローチャートを図4に示す。

【0020】IPモジュール24はフラグメント入れ替えテーブル26を有しており、IPモジュール24はフラグメント入れ替えテーブル26に基づいて通信データのフラグメンテーション及び分割されたIPデータグラム内のフラグメントオフセット値の入れ替えを行って、IPデータグラム全体の秘匿を図る。ここで、フラグメントオフセット値の入れ替え（暗号化／復号化）には、例えば対称鍵暗号系のDES（Data Encryption Standard）等の転置処理を使用する。

【0021】図10（A）にIPデータグラムのフレームフォーマットを示す。これは図7と同一であり、FLG（3ビット）はフラグメンテーションの制御に使用され、フラグメントオフセット（13ビット）はフラグメントされたデータが分割前のメッセージのどの位置を占めるのかを示す。図10（B）にフラグメント入れ替えテーブル26の一実施例を示す。同図中、IPデータサイズの下限、上限それぞれはIPデータ（即ちTCPヘッダとデータ）の長さを表す。フラグメントデータ長はオクテット単位であり、このフラグメントデータ長の最大値はネットワーク毎に設定されているMTUの最小値よりも小さい値に設定する。これはネットワークでフラグメンテーションが行われないようにするためである。なお、MTUの最小値は128オクテット程度である。暗号／復号鍵は例えば56ビット長である。

【0022】図11はデータ送信元のIPモジュール24が行う送信動作のフローチャートを示す。同図中、ステップS100でトランスポート層20から送信フレームを受信する。ステップS102で受信した送信フレームのIPデータのサイズを、フラグメント入れ替えテーブル26の各行のIPデータサイズの下限、上限と比較してチェックする。

【0023】次に、ステップS104ではフラグメント入れ替えテーブル26の該当した行のフラグメントデータ長を用いて、上記IPデータを分割し、分割した各データに昇順のフラグメントナンバーを付与する。ステッ

プS106でフラグメント入れ替えテーブル26の該当した行の暗号／復号鍵を用いて上記各データのフラグメントナンバーを暗号化する。ステップS108で次式を用いて暗号化されたフラグメントオフセットを各データについて算出する。

【0024】暗号化フラグメントオフセット＝（暗号化フラグメントナンバー）×フラグメントデータ長／8
ここで、除数の8はIP層でのフラグメンテーションの最小単位が8オクテットであり、フラグメントオフセットが8オクテットを基数とした値を取るためである。

【0025】次に、ステップS110で分割した各データと暗号化フラグメントオフセットを基にIPデータグラムを作成する。この後、ステップS112で送信先IPアドレスに含まれるネットワークアドレスと、自IPモジュールの保持しているIPアドレスに含まれるネットワークアドレスとを比較チェックして、一致すれば送信先IPアドレスと同一IPアドレスを持つデータエントリをARPキャッシュ18より検索する。

【0026】この検索で同一IPアドレスを持つデータエントリがあれば、ステップS114で送信先IPアドレスと対となるMACアドレスでイーサネットフレーム（受信フレーム）内の送信先MACアドレスを更新し、自IPモジュールの保持しているIPアドレスに対応するMACアドレスでイーサネットフレーム（受信フレーム）内の送信元MACアドレスを更新し、ステップS116でイーサネットモジュール10に送信する。

【0027】ステップS112の検索で同一IPアドレスを持つデータエントリがない場合は、ステップS118でARPモジュール16に送信先IPアドレスを送信し、ステップS120でARPモジュール16より対応する送信先IPアドレスとMACアドレスを受信したことを確認した後、ステップS122でARPモジュール16より受信したMACアドレスでイーサネットフレーム（受信フレーム）内の送信先MACアドレスを更新し、自IPモジュールの保持しているIPアドレスに対応するMACアドレスでイーサネットフレーム（受信フレーム）内の送信元MACアドレスを更新し、ステップS116でイーサネットモジュール10に送信する。

【0028】図12はエンドノードのIPモジュール24が行う受信動作のフローチャートを示す。同図中、ステップS130でイーサネットモジュール10よりIPデータグラムを受信する。ステップS132で受信フレーム内のIPアドレスと自モジュールのIPアドレスを比較し、IPアドレスが不一致の場合は、ステップS134でイーサネットフレームを破棄する。また、IPアドレスが一致していればステップS136でIPデータグラム内のモアビットを参照し、フレーム分割されているならばステップS130に進む。全フレームを受信するとステップS138からステップS138に進み、受信した全フレームからIPデータサイズを算出する。

【0029】次に、ステップS140で全フレームのIPデータサイズを、フラグメント入れ替えテーブル26の各行のIPデータサイズの下限、上限と比較してフラグメント入れ替えテーブル26の該当した行のフラグメントデータ長、及び暗号/復号鍵を確定する。ステップS142で受信した各IPデータグラムのIPデータ毎に、次式を用いて暗号化フラグメントナンバーを各データについて算出する。

【0030】(暗号化フラグメントナンバー) = 暗号化フラグメントオフセット × 8 / フラグメントデータ長
 ステップS144ではフラグメント入れ替えテーブル26の該当した行の暗号/復号鍵を用いて上記各データの暗号化フラグメントナンバーを復号化して各データのフラグメントナンバーを算出する。次に、ステップS146でフラグメンテーションにより元のデータグラムの再構築を行い、ステップS148でトランスポート層20にIPデータグラムを送信する。

【0031】ここで、図13(A)に示すような32バイトの送信フレームをトランスポート層20から受信した場合について説明する。また、ここで使用するフラグメント入れ替えテーブル26を図13(B)に示す。この場合は送信フレームのサイズがフラグメント入れ替えテーブルの第1行のIPデータサイズの下限、上限の範囲にあるため、フラグメントデータ長は8で、暗号/復号鍵は0000000000000001となる。上記のフラグメントデータ長で分割した図13(C)に示す各データに昇順のフラグメントナンバーが付与され、暗号/復号鍵を用いて図13(C)に示す各データの暗号化フラグメントナンバー及び暗号化フラグメントオフセットが得られる。

【0032】この場合、図14に示すネットワーク1のMTU(単位はオクテット)は1200、ネットワーク2のMTUは532、ネットワーク3のMTUは276であるとする。ノード発信元でオリジナルのデータグラムが1024オクテットのデータを持つ場合であっても、ノード発信元でフラグメンテーションされた図14に示す4つのIPデータグラムが送信される。

【0033】ところで、ネットワーク3を伝送される上記のIPデータグラムを例えばポイントXで第3者がモニタしたとしても、各IPデータグラムのフラグメントナンバー及びフラグメントオフセットは暗号化されたものであるため、再構築されるデータグラムはスクランブルされたものとなって、元のデータグラムを復元することはできない。つまり、通信データの秘密性を得ることができる。また、鍵を送信しないためにデータ秘密性が向上する。

【0034】エンドノードではフラグメントされた4つのIPデータグラムを受信すると、受信した全てのIPデータサイズ(32バイト)で図15(A)に示すフラグメント入れ替えテーブル26を参照し、全てのIPデ

ータサイズ(32バイト)がフラグメント入れ替えテーブルの第1行のIPデータサイズの下限、上限の範囲にあるため、フラグメントデータ長は8で、暗号/復号鍵は0000000000000001であると確定する。

【0035】この後、式(暗号化フラグメントナンバー) = 暗号化フラグメントオフセット × 8 / フラグメントデータ長を用いて各データの暗号化フラグメントナンバーを図15(B)に示すように算出し、この暗号化フラグメントナンバーを暗号/復号鍵図15(B)に示す各データのフラグメントナンバーを復元する。そして、このフラグメントナンバーを用いてフラグメンテーションを行い元のデータグラムを復元する。

【0036】次に、公衆データ網に接続されたパケットモードで動作するデータ端末装置(DTE)とデータ回線終端装置(DCE)間のインタフェースプロトコルであるX.25に適用した実施例について説明する。X.25ではパケットの分割/統合はデータリンク層で行われる。送信側X.25ゲートウェイのデータリンク層で図16(C)に示すようなIPデータが576オクテットの送信フレームをIP層から受信した場合、データリンク層でデフォルトでは128オクテットの5つのパケットに分割する。本発明では、データリンク層で図16(A)に示すフラグメント入れ替えテーブルを使用し、この場合、送信フレームのサイズがフラグメント入れ替えテーブルの第3行のデータサイズの下限、上限の範囲にあるため、分割データ長は64(オクテット)で、暗号/復号鍵は0000000000000003となる。

【0037】576オクテットの送信フレームを分割データ長の64オクテットで図16(B)に示す9個のパケットに分割した場合、各送信X.25フレームの制御フィールドの送信順序番号N(S)、受信順序番号N(R)のうちN(S)の初期値は分割の順序に付与される。この送信順序番号N(S)、受信順序番号N(R)を暗号/復号鍵を用いて暗号化し、暗号化送信順序番号N(S)、暗号化受信順序番号N(R)が得られる。この暗号化を行わない場合には図17に示す各送信X.25フレームがネットワークに送信されるが、本発明では図18に示す各送信X.25フレームがネットワークに送信される。両者では送信順序番号N(S)、受信順序番号N(R)が異なっており、図18では、そのうちの送信順序番号N(S)を示している。なお、X.25フレームは基本モード(モジュロ8)で、Fはフラグシーケンス、Aはアドレスフィールド、Cは制御フィールド、FCSはフレームチェックシーケンスである。

【0038】ところで、ネットワークを伝送された図18の送信X.25フレームを第3者がモニタしたとしても、各送信X.25フレームでは暗号化送信順序番号N(S)、暗号化受信順序番号N(R)を使用しているため、再構築されるデータフレームはスクランブルされたものとなって、元のデータフレームを復元することはで

きない。つまり、通信データの秘匿性を得ることができる。また、鍵を送信しないためにデータ秘匿性が向上する。

【0039】受信側X、25ゲートウェイのデータリンク層では物理層から受信したX、25フレームのデータ部(パケット)のデータ長(64)で図19(A)に示すフラグメント入れ替えテーブルを参照し、データ長64オクテットがフラグメント入れ替えテーブルの第3行のデータサイズの下限、上限の範囲にあるため、暗号/復号鍵は0000000000000003であると確定する。

【0040】この後、暗号/復号鍵を用いて図19(B)に示す受信した各X、25フレームの暗号化送信順序番号N(S)、暗号化受信順序番号N(R)を復号し、元の送信順序番号N(S)を得る。そして、この送信順序番号N(S)、受信順序番号N(R)を用いて図19(C)に示す元のデータフレームを復元してIP層に送信する。なお、送信順序番号N(S)、受信順序番号N(R)の復号後、所定のN(S)、N(R)のチェックで異常を検出した場合は、受信側X、25ゲートウェイのデータリンク層の動作により、制御フィールドの送信順序番号N(S)、受信順序番号N(R)を交換した再送信要求フレームを送信して再送信要求を行う。

【0041】なお、ステップS102~S110が暗号化手段に対応し、ステップS138~S144が復号化手段に対応する。

【0042】

【発明の効果】上述の如く、請求項1に記載の発明は、送信側の端末に、通信データを所定データ長に分割し、前記分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して前記分割データそれぞれに付加しネットワークに送出する暗号化手段を設け、受信側の端末に、前記ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を前記所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って前記受信した分割データから元の通信データを復元する復号化手段を設け、前記ネットワーク上で通信データの内容を秘匿する。

【0043】このように、通信データを所定データ長に分割し、分割データそれぞれの順序またはオフセットを示す数値を所定の鍵を用いて暗号化して分割データそれぞれに付加しネットワークに送出し、ネットワークから受信した分割データそれぞれに付加されている暗号化された数値を所定の鍵を用いて復号化し、復号化した数値の示す順序またはオフセットに従って受信した分割データから元の通信データを復元するため、ネットワーク上で通信データをモニタしたとしても、この通信データが所定データ長でスクランブルされており、通信データ全体の内容を知ることができず、通信データの内容を秘匿できる。

【0044】また、請求項2に記載の発明は、暗号化手段及び復号化手段で用いる所定の鍵は、前記通信データのデータ長に対応して決定する。このように、所定の鍵を通信データのデータ長に対応して決定するため、送信側、受信側それぞれで同一の鍵を用いて暗号化、復号化を行うことができ、かつ、鍵を送信しないためにデータ秘匿性が向上する。

【0045】また、請求項3に記載の発明は、通信データを分割する所定データ長は、前記通信データのデータ長に対応して決定する。このように、所定データ長を通信データのデータ長に対応して決定するため、受信側では受信した分割データのデータ長から一意に復号化の鍵を知ることができる。

【0046】また、請求項4に記載の発明は、送信側及び受信側の端末は、TCP/IPプロトコルに基づいてネットワークと通信を行う。これによって、TCP/IPプロトコルの通信において通信データの秘匿性を得ることができる。また、請求項5に記載の発明は、送信側及び受信側の端末は、X、25プロトコルに基づいてネットワークと通信を行う。

【0047】これによって、X、25プロトコルの通信において通信データの秘匿性を得ることができる。

【図面の簡単な説明】

【図1】従来方式のTCP/IPをサポートした端末の機能ブロック図である。

【図2】イーサネットモジュール10の動作フローチャートである。

【図3】ARPキャッシュ18の構成を示す図である。

【図4】ARPモジュール16の動作フローチャートである。

【図5】IPモジュール14の動作フローチャートである。

【図6】イーサネットモジュール10の動作フローチャートである。

【図7】イーサネットフレームのIPデータグラムのフレームフォーマットを示す図である。

【図8】従来のネットワークにおけるフラグメンテーションを説明するための図である。

【図9】本発明の通信データ秘匿方式を適用したTCP/IPをサポートした端末の機能ブロック図である。

【図10】本発明方式を説明するための図である。

【図11】データ送信元のIPモジュール24が行う送信動作のフローチャートである。

【図12】エンドノードのIPモジュール24が行う受信動作のフローチャートである。

【図13】本発明方式を説明するための図である。

【図14】本発明方式を説明するための図である。

【図15】本発明方式を説明するための図である。

【図16】本発明方式をX、25に適応した実施例について説明するための図である。

【図17】本発明方式をX.25に適応した実施例について説明するための図である。

【図18】本発明方式をX.25に適応した実施例について説明するための図である。

【図19】本発明方式をX.25に適応した実施例について説明するための図である。

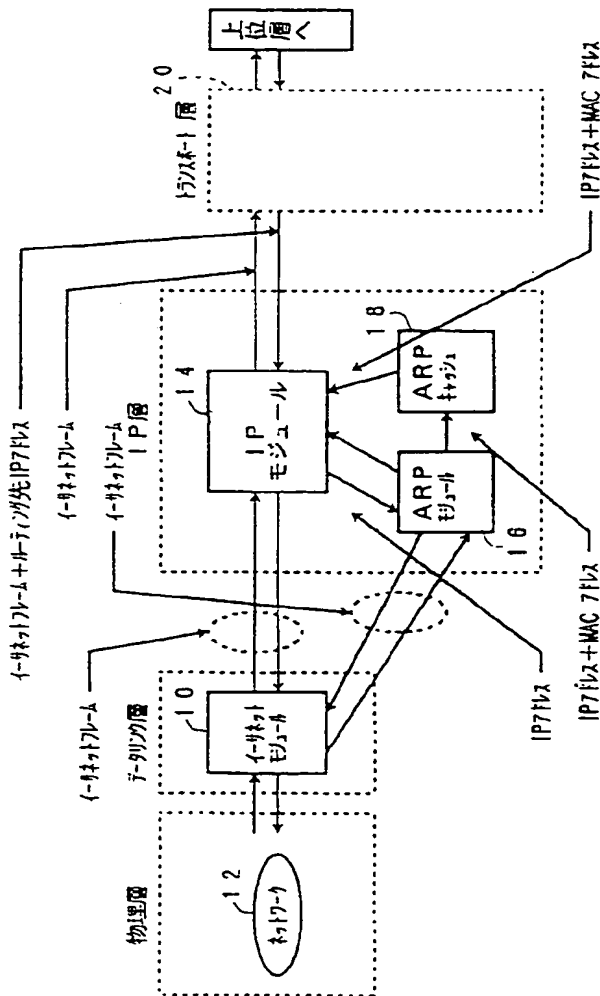
【符号の説明】

- 10 イーサネットモジュール
12 ネットワーク
16 ARPモジュール
18 ARPキャッシュ
20 トランスポート層
24 IPモジュール

【図1】

【図3】

従来方式のTCP/IPをサポートした端末の機能ブロック図



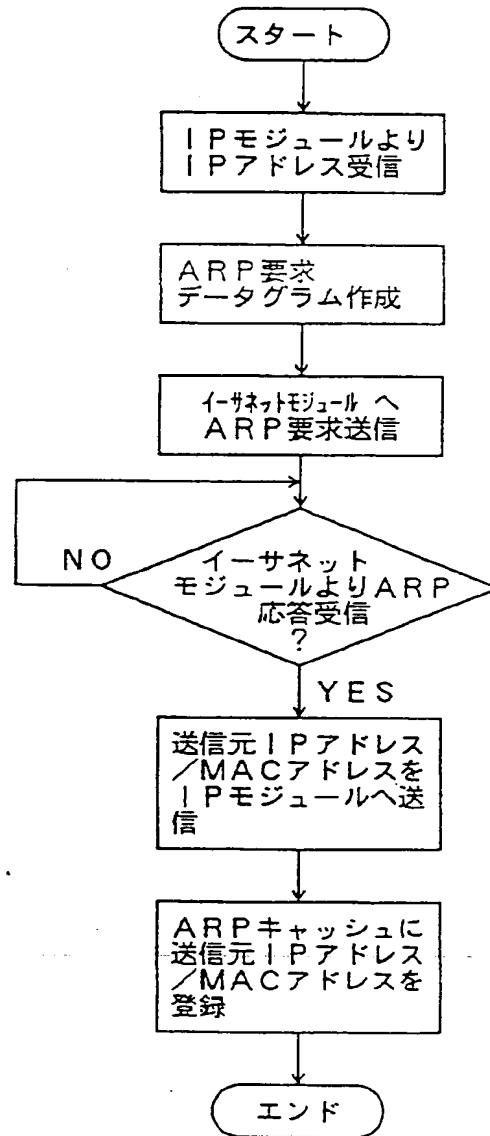
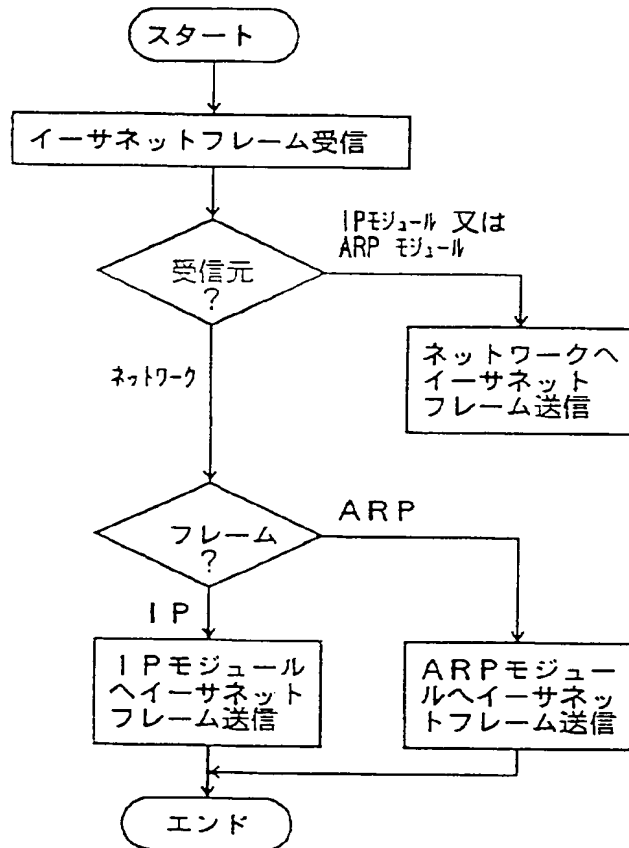
ARPキャッシュ18の構成を示す図

IPアドレス	MACアドレス
160.1.1.1	0A-08-0C-00-10-01
160.1.1.2	0A-08-0C-00-10-02
160.1.1.3	0A-08-0C-00-10-03
⋮	⋮

【図2】

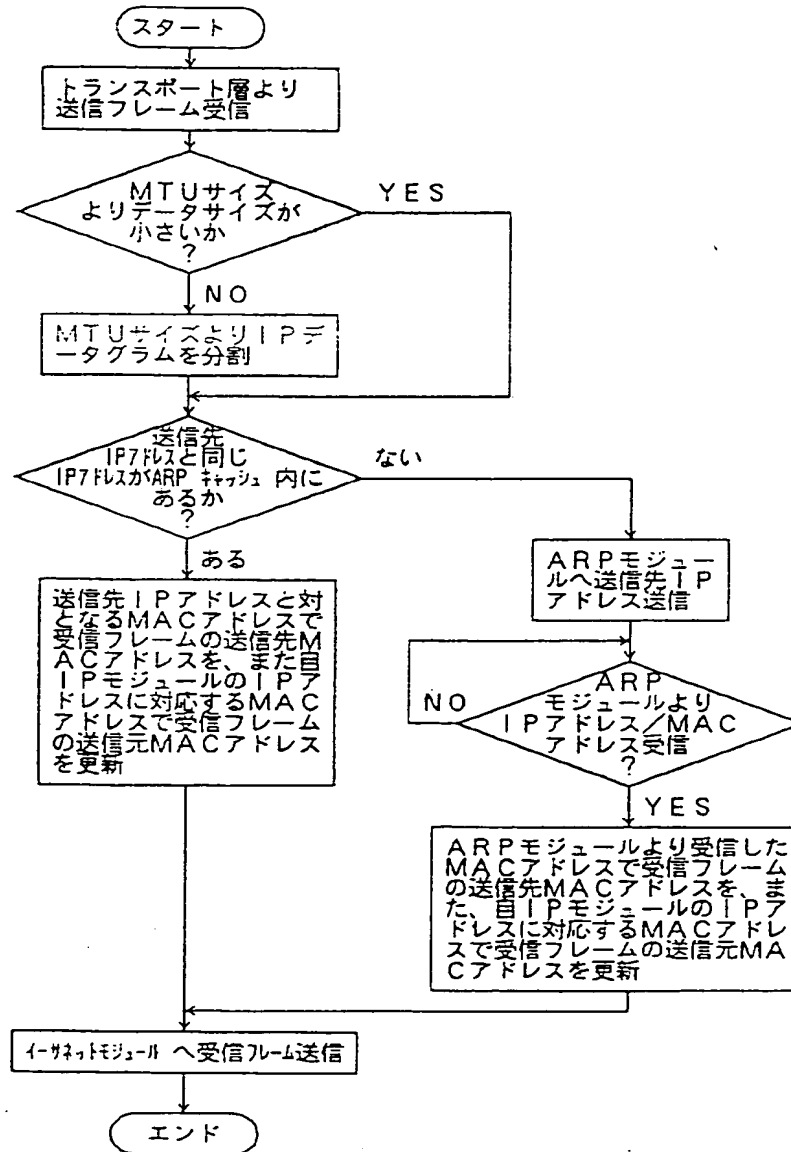
【図4】

イーサネットモジュール10の動作フローチャート ARPモジュール16の動作フローチャート



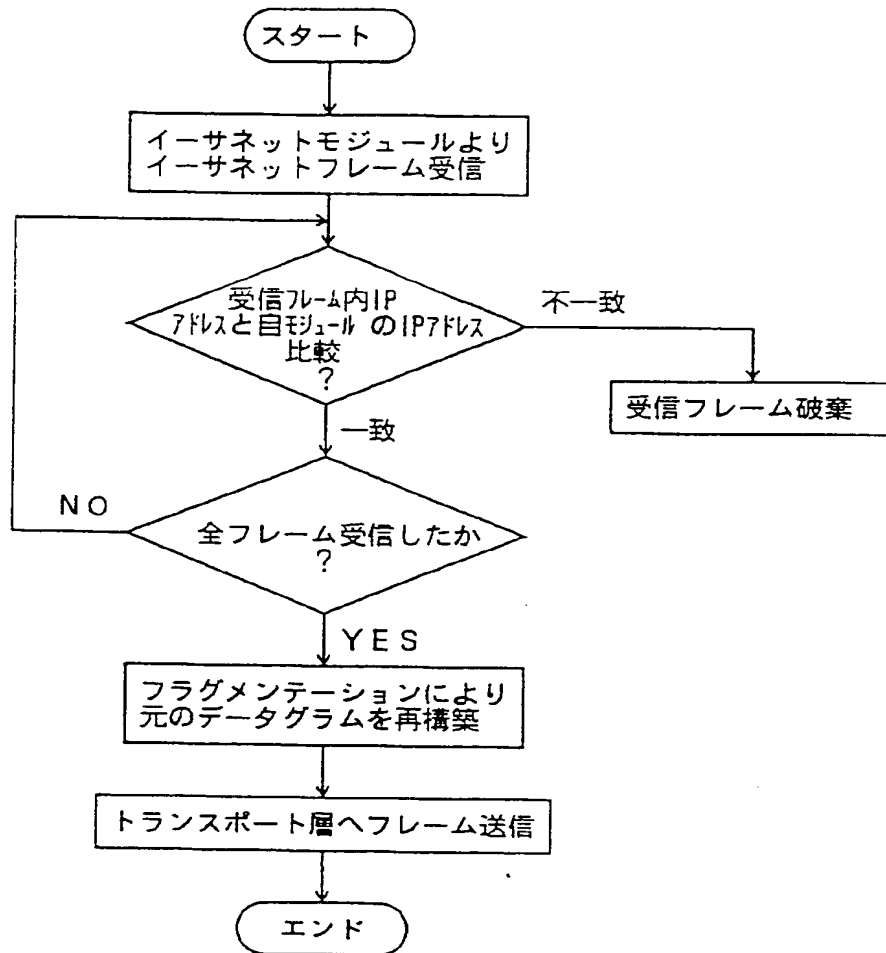
【図5】

IPモジュール14の動作フローチャート



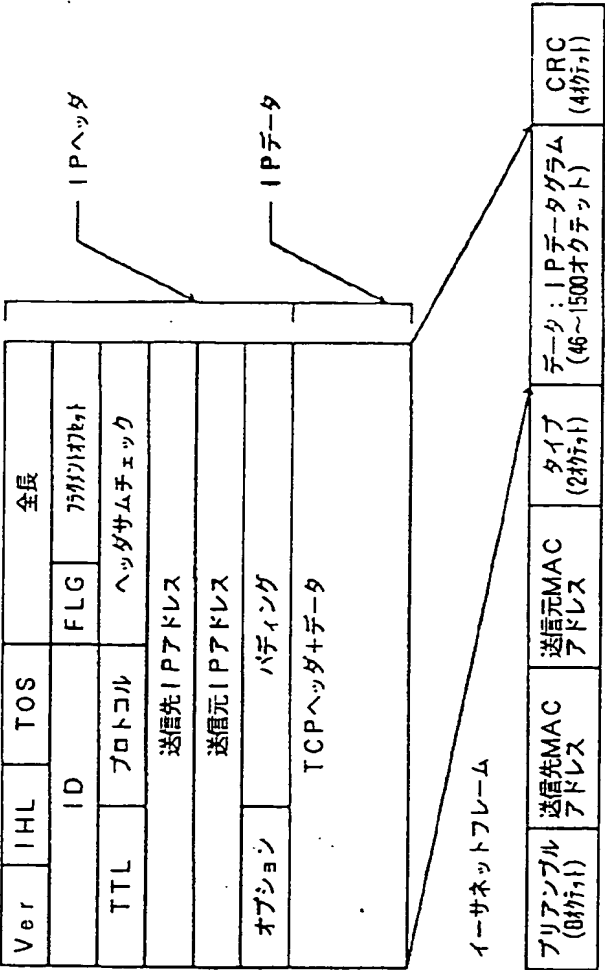
【図6】

イーサネットモジュール10の動作フローチャート



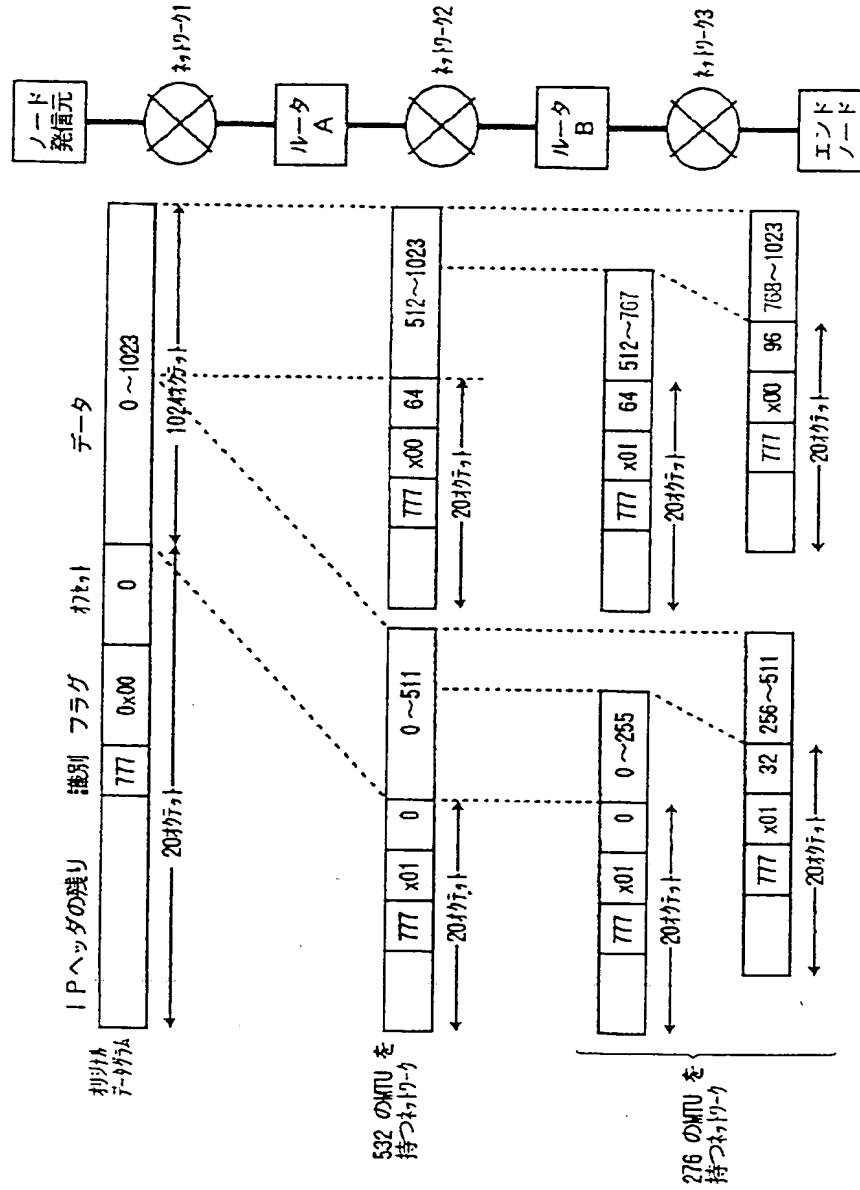
【図7】

イーサネットフレームのIPデータグラムのフレームフォーマットを示す図



【図8】

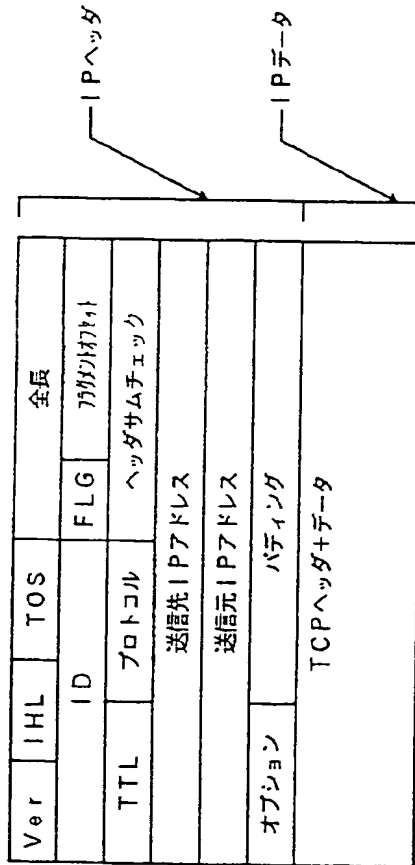
従来のネットワークにおけるフラグメンテーションを説明するための図



【図10】

本発明方式を説明するための図

(A)

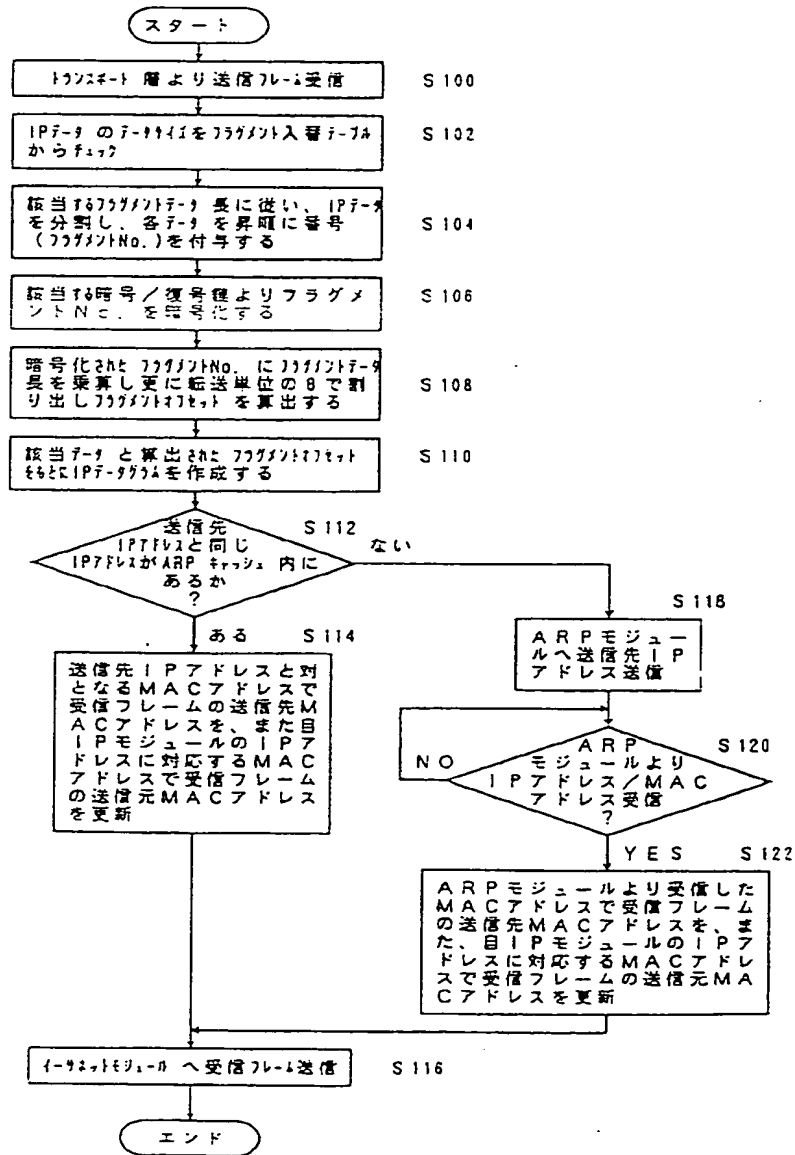


(B)

IPアドレス下限	IPアドレス上限	オフセット長	暗号/復号鍵 (56ビット)	備考
0	256	8	0000000000000001	
257	512	16	0000000000000002	
513	1024	32	0000000000000003	
.	.	.	.	
.	.	.	.	

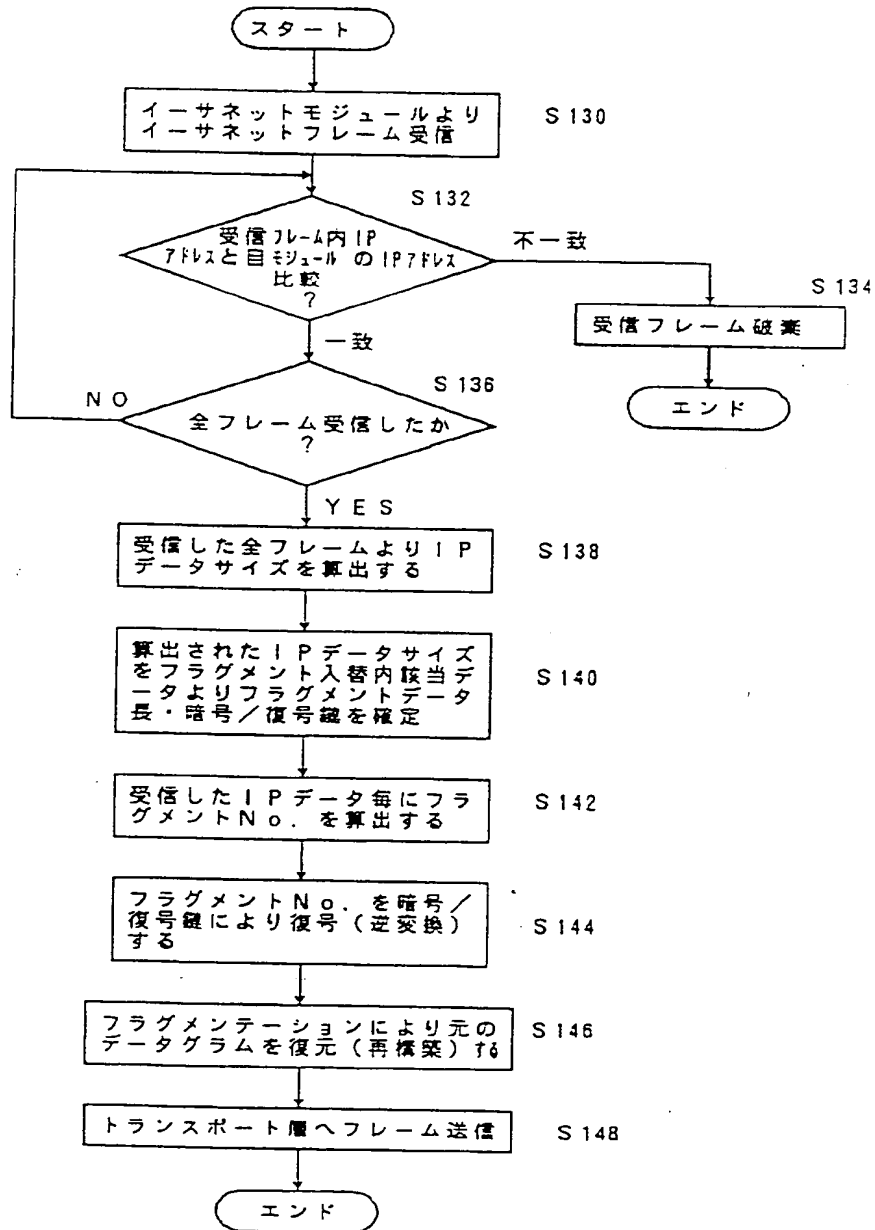
【図11】

データ送信元のIPモジュール24が行う送信動作のフローチャート



【図12】

エンドノードのIPモジュール24が行う受信動作のフローチャート



【図13】

本発明方式を説明するための図

0102030405060708091011121314151617181920212223242526272829303132					
← 32バイト →					

(A)

IPデータ下限	IPデータ上限	フラグメント長	暗号/復号鍵 (56ビット)	備考
0	256	8	0000000000000001	
257	512	16	0000000000000002	
513	1024	32	0000000000000003	
.	.			
.	.			

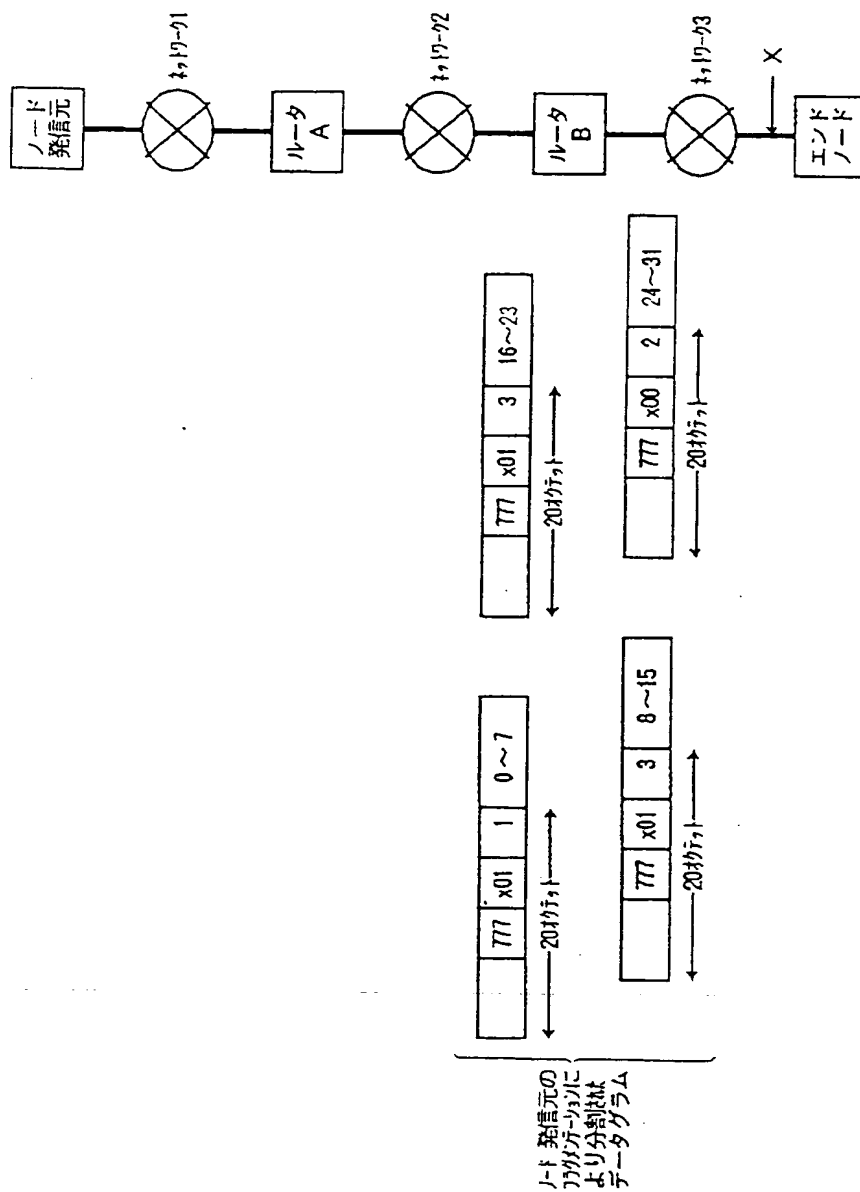
(B)

分割されたIPデータ列	フラグメント No. 初期値	暗号/復号化による暗号化	暗号化したフラグメント No.	暗号化したフラグメント
0102030405060708	0	↑	1	1
0910111213141516	1		3	3
1718192021222324	2		0	0
2526272829303132	3		2	2

(C)

【図14】

本発明方式を適用するための図




【図15】

本発明方式を適用するための図

(A)

IPデータ下限	IPデータ上限	ワザンデータ長	暗号／復号鍵 (56ビット)	備考
0	256	8	0000000000000001	
257	512	16	0000000000000002	
513	1024	32	0000000000000003	
.	.			
.	.			

(B)

分割されたIPデータ列	暗号化されたワザンビット	暗号化されたワザンNo.	暗号／復号鍵による復号化	指示されたワザンNo.
0102030405060708	1	1		0
0910111213141516	3	3		1
1718192021222324	0	0		2
2526272829303132	2	2		3

【図16】

本発明方式をX. 25に適應した実施例について説明するための図

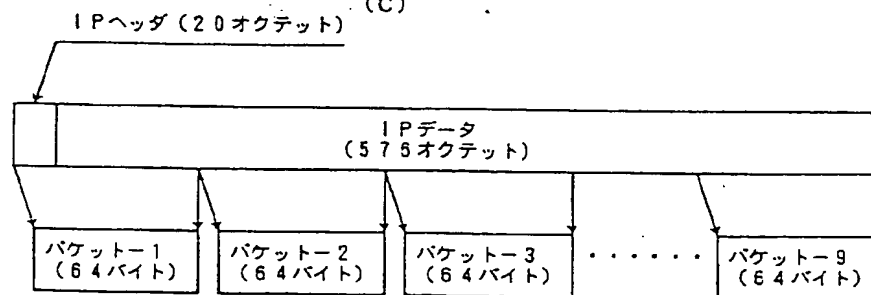
(A)

IPヘッダサイズ下限	IPヘッダサイズ上限	分割データ長	暗号/復号鍵 (56ビット)	備考
0	256	16	0000000000000001	
257	512	32	0000000000000002	
513	1024	64	0000000000000003	
.	.			
.	.			

(B)

送信X. 25フレーム	制御フィールド (N (S))	暗号/復号鍵による暗号化	暗号化した制御フィールド (N (S))
X. 25フレーム-1	0	→	8
X. 25フレーム-2	1		7
X. 25フレーム-3	2		6
X. 25フレーム-4	3		5
X. 25フレーム-5	4		4
X. 25フレーム-6	5		3
X. 25フレーム-7	6		2
X. 25フレーム-8	7		1
X. 25フレーム-9	8		0

(C)



【図19】

本発明方式をX. 25に適應した実施例について説明するための図

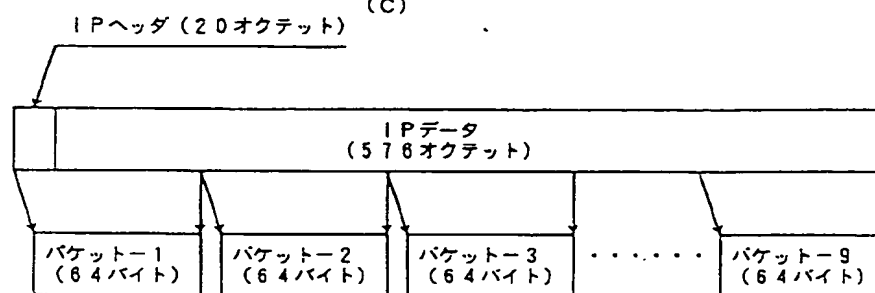
(A)

IPヘッダサイズ下限	IPヘッダサイズ上限	分割データ長	暗号/復号鍵 (56bit)	備考
0	256	16	00000000000001	
257	512	32	00000000000002	
513	1024	64	00000000000003	
.	.			
.	.			

(B)

送信X. 25フレーム	暗号化した制御フィールド (N(S))	暗号/復号鍵による暗号化	制御フィールド (N(S))
X. 25フレーム-1	8	→	0
X. 25フレーム-2	7		1
X. 25フレーム-3	6		2
X. 25フレーム-4	5		3
X. 25フレーム-5	4		4
X. 25フレーム-6	3		5
X. 25フレーム-7	2		6
X. 25フレーム-8	1		7
X. 25フレーム-9	0		8

(C)



フロントページの続き

(72)発明者 平山 裕之
神奈川県川崎市高津区坂戸3丁目2番1号
富士通ネットワークエンジニアリング株
式会社内

Fターム(参考) 5K013 BA02 CA07 FA06
5K030 GA15 HA06 HA08 HC01 JA05
KA19 LA08 LD19
5K032 AA08 BA14 CC09 CC11

THIS PAGE BLANK (USPTO)